TN Department of General Services

MEMO

# SWC# 3021 Comprehensive Cloud Solutions Contract Information and Usage Instructions

**Specific instructions for STS workstation consolidated executive branch agencies, non-consolidated executive branch agencies, and local governments are broken out below on pages 3, and 5, and 6.**

**Summary**

Statewide contract 3021 is a NASPO cooperative contract between the State of Tennessee and four suppliers: Carahsoft, Insight, Strategic Solutions and SHI.

The scope of offerings includes Software-as-a-Service (Saas), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) solutions including, but not limited to Amazon Web Services, Google Cloud Platform, and Microsoft Azure. Cloud professional services such as fixed-deliverable projects, application managed services, cloud solution assessments, or training for applicable solutions are also included. The following table shows which supplier offers which platform:

| | AWS | GCP | Azure |
|---|---|---|---|
| Carahsoft | ● | ● | |
| Insight | ● | | ● |
| SHI | ● | ● | ● |
| Strategic | ● | ● | ● |

**Contract Period:**

| | Carahsoft | Insight | Strategic | SHI |
|---|---|---|---|---|
| Start Date | 9/1/2020 | 9/14/2020 | 5/23/2023 | 9/21/2020 |
| End Date with All Renewals Executed | 8/31/2025 | 9/13/2025 | 9/15/2026 | 9/20/2025 |

**State Contact Information**

**Contract Administrator**
Michael D. Gross, Category Specialist
Central Procurement Office
Michael.D.Gross@tn.gov
(615) 507-6227

**Strategic Technology Solutions Contact**
Chris Benson, Director of Business Operations
Strategic Technology Solutions
Chris.Benson@tn.gov
(615) 770-1126

**Supplier Contact Information**

| **Company Name: Carahsoft** |
|---|
| Master Agreement #: AR2472 |
| Edison Contract Number: 67955 |
| Supplier Number: 703 |

**Quote requests:** NASPO@carahsoft.com
**SOW requests:** SMGNASPO@carahsoft.com

Colby Bender, Team Lead, Contracts Team
Colby.Bender@Carahsoft.com
(703) 889-9878

| **Company Name: Insight** |
|---|
| Master Agreement #: AR2485 |
| Edison Contract Number: 67958 |
| Supplier Number: 529 |

**Quote requests:** TeamAshley2@insight.com

Ashley McDonald, Account Executive, Field Sales
Ashley.McDonald@Insight.com
(423) 368-9042

| **Company Name: Strategic Communications** |
|---|
| Master Agreement #: AR2490 |
| Edison Contract Number: 78633 |
| Supplier Number: 269788 |

**Quote requests:** naspo@yourstrategic.com
Justin Hampton, Account Executive
844-243-2053

| **Company Name: Software House International (SHI)** |
|---|
| Master Agreement #: AR2488 |
| Edison Contract Number: 67960 |
| Supplier Number: 12676 |

**Quote requests:** SoutheastTeamgov@shi.com

Nick Porco, Account Executive
Nick_porco@shi.com
629-401-8746

Inside Team Distribution:
Ryan Lee, Account Executive
ryan_lee@shi.com
615-390-2836

Lexi Ettman,
Inside Account Manager
lexi_ettman@shi.com
800-715-6055

**Offerings**
Each supplier has a reseller list which shows offerings that are currently available. These can be found on the NASPO websites listed below:

- Carahsoft – https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/carahsoft-technology-corporation/
- Insight - https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/insight-public-sector-inc/
- Strategic Communications - https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/strategic-communications-llc/
- SHI - https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/shi-international-corp/

*Always ask each of the four suppliers for quotes to ensure the best price.*

## INSTRUCTIONS FOR STS WORKSTATION CONSOLIDATED EXECUTIVE BRANCH AGENCIES

If you wish to purchase a cloud solution not found on price lists, please contact Chris Benson at STS Business Operations with the request. STS Business Operations will review the request and work with the Contract vendors to determine if the requested solution is available through this contract.

**ServiceNow**
All purchases from these contracts must be purchased through ServiceNow unless prior written authorization received from Chris Benson or Emily Gibson to procure directly in Edison (see link below). https://tn.service-now.com/sp?id=sc_cat_item&sys_id=8775167a13826a009f84b6246144b071

An STS Endorsement is required if your agency has not procured the specific offering at some point in the past.

If you have an interest in purchasing Infrastructure-as-a-Service through this contract, please contact **CloudTN@tn.gov** or IT consolidated agencies may request a consultation with the CloudTN team through the ServiceNow request, "**CloudTN Consultation**".

**Statements of Work**
Please use a statement of work (SOW) when your purchase includes customized professional services. We have created a SOW template for your use, see Attachment 1 below.

**Pick List**
This contract features robust security language pertaining to the cloud hosting of State data. Different contract terms have been added to cover specific data-hosting security requirements. Different terms apply depending on which type of data is being hosted. Because of this, the type of data being hosted and therefore which contract term is applicable must be clearly laid out *at the order level*. This can be achieved either in a SOW or printed on to the purchase order directly if no SOW is being used. STS Information Security will review the type(s) of data being hosted and will designate what additional applicable terms and conditions will apply to the purchase.

**EULA Rider**
Please be aware that when ordering from a new publisher, the supplier may require the State to agree to an End User License Agreement or other terms and conditions as part of the order. If the supplier

requires the State to agree to additional terms and conditions for the order,  a EULA Rider may need to be negotiated. Negotiations will be conducted between CPO Legal and the software publisher in question. Please email Michael Gross if this need arises. A EULA Rider template is included below as Attachment 2 for reference.

**Justification**

When entering your Edison requisition or ServiceNow procurement request for any order placed against this contract please attach brief justification documentation for audit purposes. Justification should include an explanation of the business need(s) being met by the requested solution and a description of the research the procuring agency performed to support the selection of the requested solution.

**Software Waiver / Exception Process**

Follow the steps below to request a waiver or exception to a cloud-based software (Software as a Service, SaaS) standard included in the Tennessee Enterprise Architecture.

1. Download the Waiver/Exception Request form here: https://www.teamtn.gov/sts/planning-services/information-systems-planning/waiver---exception-process.html
2. Complete the form electronically.
3. Email the completed form to AG_Standard_Products_List@tn.gov along with any additional information needed to support the Exception Request.

## INSTRUCTIONS FOR NON-STS WORKSTATION CONSOLIDATED EXECUTIVE BRANCH AGENCIES

Please contact the Contract vendors directly to inquire about the availability of a cloud solution for resale.

If you have an interest in purchasing Infrastructure-as-a-Service through this contract, please contact **CloudTN@tn.gov**.

### Statements of Work

Please use a statement of work (SOW) when your purchase includes customized professional services. We have created a SOW template for your use, see Attachment 1 below.

### Pick List

This contract features robust security language pertaining to the cloud hosting of State data. Different contract terms have been added to cover specific data-hosting security requirements. Different terms apply depending on which type of data is being hosted. Because of this, the type of data being hosted and therefore which contract term is applicable must be clearly laid out *at the order level*. This can be achieved either in a SOW or printed on to the purchase order directly if no SOW is being used.

### EULA Rider

Please be aware that when ordering from a new publisher, an End User License Agreement (EULA Rider) may need to be negotiated. Negotiations will be conducted between CPO Legal and the software publisher in question. Please email Michael Gross if this need arises. A EULA Rider template is included below as Attachment 2 for reference.

### Justification

When entering your Edison requisition for any order placed against this contract please attach brief justification documentation for audit purposes. Justification should include an explanation of the business need(s) being met by the requested solution and a description of the research the procuring agency performed to support the selection of the requested solution.

## INSTRUCTIONS FOR LOCAL GOVERNMENTS

Please contact the Contract vendors directly to inquire about the availability of a cloud solution for resale.

### Statements of Work

We have created a SOW template for State agencies to use in the event their purchase includes customized professional services. You may be able to modify this template for your uses if you so wish - see Attachment 1 below.

### Pick List

This contract features robust security language pertaining to the cloud hosting of State data. Different contract terms have been added to cover specific data-hosting security requirements. Different terms apply depending on which type of data is being hosted. Because of this, the type of data being hosted and therefore which contract term is applicable must be clearly laid out *at the order level*. This can be achieved either in a SOW or printed on to the purchase order directly if no SOW is being used.

### EULA Rider

Please be aware that when ordering from a new publisher, an End User License Agreement (EULA Rider) may need to be negotiated. We have created a EULA Rider template for State agencies if the need arises. You may be able to modify this template for your uses if you so wish - see Attachment 2 below.

**<u>Attachment 1</u>**

**Statement of Work Template**

# *[Insert Contract Number and Name]*

## *[Insert Requesting State Agency name]*

# Statement of Work

## For

## *[Insert Project Title]*

## *[Insert Planview Work ID - Sequential #]*

## *[Date]*

# 1.0 Statement of Work

## 1.1 *Project Title*

This Statement of Work (SOW) is being executed between *[insert Contractor name]* ("Contractor") and *[Insert Agency]* ("Agency" or "Purchasing Entity") for [*insert a brief description of the project*], effective as of *[Insert Effective Date]* (the "SOW Effective Date").

This Statement of Work (SOW) constitutes an Order under that certain *[Contract or Participating Addendum]* between *[contractor name]* and the State of Tennessee, *[contract name and number]*, (the "Contract") and incorporates by reference the terms and conditions, specifications, and other incorporated contract documents of the Contract. In case of any conflict between this SOW and the Contract, the Contract shall prevail.

## 1.2 Background

- *Describe the history of your project and the prior events that brought you to this SOW*

## 1.3 Reference to other applicable documents

The following documents are hereby incorporated by reference into this SOW:

- *List any pertinent documents or supporting materials pertaining to the SOW, if any, otherwise write "None".*

## 1.4 General Security Requirements – Pick List

- □ Confidential State Data
- □ Confidential Data Housed in the United States
- □ Confidential State Data Encrypted at Rest using FIPS
- □ Annual Penetration Tests and Vulnerability Assessment of Processing Environment
- □ Contractor Supplied Copy of State Confidential Data it is Housing
- □ Upon request after termination of the contract, Destruction of State Confidential Data
- □ FTI Data – requires IRS Publication 1075
- □ CMS Data and MARS-E controls
- □ PCI and PCI DSS controls
- □ CJIS Data – Must consult TBI first
- □ HIPAA Data – Must include a BAA
- □ Confidential State Date Processing Environment:
- □ ISO 27001 and FedRAMP
- □ AICPA and SOC II

## 2.0 AGENCY STAFFING AND ROLES

### 2.1 Staffing

Project Manager – Agency
The Agency's Project Manager is:

*Name:*
*Address:*
*City:*
*State & Zip*
*Phone:*
*Cell:*
*Fax:*
*Email:*

*Insert contact information for any additional relevant staff.*

### 2.2 Agency Staff and Roles

- *Who within the agency will have decision-making authority, including approval of changes, report, documentation and deliverables?*
- *State agency staff (if any) to assist with the project effort*
- *Individuals key to the project and detail their roles and responsibilities*

## 3.0 PROJECT REQUIREMENTS AND DELIVERABLES

### 3.1 Requirements

*Describe:*

- *Tasks to be performed  and any additional Contractor qualifications for specialized projects*
- *Any known non-standard work schedule tasks*
- *Location(s) where project work is required to be performed or may be performed, including the use of onsite, offsite, and offshore resources at the procuring State agency's discretion*
- *Include tasks that do not result in specific deliverables (i.e. project management)*
- *Include any security requirements from Special Terms and Conditions, Section 13 of the Contract that are applicable to this SOW.*

### 3.2 Agency Tasks and Responsibilities

- *Include tasks to be performed by the agency*
- *Precise definition of all hardware, software, data services, and facilities the agency will provide*

### 3.3 Deliverables

*Describe the Deliverables to be provided under this SOW, including the estimated delivery dates. If no Deliverables, state "none.*

### 3.4 Exclusions

*Describe:*

- *Tasks which are not part of the scope of this project*

## 4.0 Cost Criteria

### 4.1 Payment Methodology

*Describe the payment methodology and the associated charges applicable to this SOW.*

### 4.2 SOW Monetary Cap

Check one of the following to apply to this SOW:

□ This SOW is a fixed fee SOW. The total charges under this SOW is *[_________]* dollars *($___) [specify SOW monetary cap]* for the performance of the work as set forth in this SOW.

□ This SOW is a time and materials SOW. The total charges under this SOW is *[_________]* dollars *($___) [specify SOW monetary cap]* for the performance of the work as set forth in this SOW (the "SOW NTE Amount"). The Agency shall compensate the Contractor for actual work performed, in an amount not to exceed the SOW NTE Amount. The Agency shall not be obligated to pay for, and the Contractor shall not be obligated to perform, work under this SOW in excess of the SOW NTE Amount unless and until the parties execute a written amendment to this SOW to increase such SOW NTE Amount.

□ This SOW is a consumption-based SOW. The estimated charges under this SOW is *[_________]* dollars *($___) [specify SOW estimated budget]*. For clarity, the terms of this SOW and the Contract will continue to apply to any Cloud Services provided in excess of the specified estimated charges.

### 4.3 State Agency Billing Address

*Insert the applicable State Agency billing address.*

## 5.0 Deliverable Acceptance

*Define the process for submitting, approving and rejecting deliverables (including testing dates and scenarios)*

## 6.0 Estimated Timeline and Period of Performance

Project must begin no later than *[Month, Year]* and be completed by *[Month, Year]*.

## 7.0 PROJECT MANAGEMENT (*IF APPLICABLE*)

*Describe what will be required as far as project management, which reports will be required, how often these reports will be required, and what must be submitted to the State procuring agency.*

## 8.0 ADDITIONAL STATE POLICIES AND STANDARDS

*Specifically reference any additional state policies and standards that would apply, to the extent applicable to Contractor in its performance of the work under the Order. If none, write "none".*

- *Insert any other relevant links to the latest versions of the policies, standards and environment*

## 9.0 KEY ASSUMPTIONS

*Identify any additional agency or contractor assumptions*

*If additional sections are required for your specific project, please leave the above section numbering as it is and add your new sections here as 10.0, 11.0 etc.*

This SOW will not be effective, and Contractor shall not commence services hereunder, until it is approved and signed by Contractor and the Participating Entity.
In witness whereof, the parties have executed this SOW as of the last date of execution of the signatories below.

| | |
|---|---|
| *[Insert State Purchasing Agency]* | *[Contractor Name]* |
| Signature: | Signature: |
| Name: | Name: |
| Title: | Title: |
| Date: | Date: |

**Attachment 2**

**STATE AGENCIES: PLEASE CONSULT CPO BEFORE USING THIS DOCUMENT**

The terms and conditions of this addendum (“Rider”) shall supplement the EULA (as defined below) between ________________, the licensor and provider (“Licensor”), and the State of Tennessee (including any agency, office, or commission), as licensee (“State” or “Licensee”), and are applicable to any procurement of Software, Cloud Services, and associated services from Licensor sold, licensed, transferred or otherwise provided to the State by Licensor or through a third-party reseller (“Reseller”) under the terms and conditions of SWC 3021 NASPO Cloud Solutions (“Contract”). As used in this Rider, “party” refers to Licensor or Licensee (i.e., does not include a Reseller), individually, and “parties” means the Licensor and the Licensee, collectively.
The parties agree as follows:

## 1. Additional Definitions

“Cloud Services” mean any services available via a remote cloud computing server rather than an on-site server, managed by a third party, that provide users with access to computing services such as analytics, networking, or storage via the internet.

“EULA” means any agreements between Licensor and Licensee that governs Licensee’s use of Software purchased under the Contract.

“Software” means is any set of machine-readable instructions provided to the State by or through Licensor that directs a computer’s processor to perform specific operations.

“Service Level Agreement” or “SLA” means the term setting forth the service levels that Licensor must meet in providing the Software.

## 2. Order of Precedence

This Rider takes precedence over any provision in the EULA or in any separate agreement between the Licensor and the State. In the event of a conflict between this Rider and the EULA, the Rider will prevail. Defined terms in this Rider or in the EULA will be given their ordinary meaning in this Rider as the context requires.

## 3. Term and Survival

3.1 The term of this Rider shall be concurrent with the term of the EULA.

3.2 All provisions of this Rider that should by their nature survive termination shall survive, including, Sections 5 (Limitation of Liability), 7 (Indemnification for Intellectual Property Infringement, 11 (Governing Law; Jurisdiction and Venue; ), (Fees), 14 (Warranties), and 15 (Miscellaneous).

## 4. Authorized Users

The authorized user of the Software is the State, including its employees, authorized agents, consultants, auditors, other independent contractors, or any external users contemplated by the parties. This Section does not modify the quantity of users licensed.

## 5. General License Terms

The Licensor grants a license to the State to use all Software provided under this Contract in the course of the State's business and purposes during the Term, subject to the terms of this Rider and the EULA. This paragraph does not modify the quantity of users or devices licensed. Licensor represents and warrants that the Software provided under the EULA will function: (i) as set forth in the EULA; (ii) in accordance with any agreed upon service levels; and (iii) in accordance with any documentation associated with the Software. SLA claims will not be deemed to be waived by the passage of time or the State's failure to report an issue.

The State may copy the Software only for: (a) disaster recovery and back-up purposes, and (b) installation of any personal computer Software authorized in accordance with this Rider. All copies remain the property of the Licensor. The State may deliver a copy of the Software to a disaster recovery contractor to perform temporary disaster recovery work for the State.

Title to the Software and its documentation remains with Licensor and its third-party providers of Software at all times.

## 6. Warranties

6.1 Software and Cloud Services. Licensor represents and warrants that the Software and Cloud Services provided under the EULA or this Rider will function in accordance with the documentation made available by the Licensor to the State.

6.2 Intellectual Property. Licensor represents and warrants that it has the rights necessary to license the Software or provide Cloud Services to the State in accordance with the terms of the EULA and this Rider.

6.3 Malware. Licensor warrants that the Software and Cloud Services contain no: (i) viruses, worms, spyware or malware; (ii) coding that may disable the Software or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numerals, or other similar self-destruct mechanisms (e.g., "time bombs," "time locks," or "drop dead" devices); or (iii) coding that would permit the Licensor, or any third party to access the Software to cause disablement or impairment (e.g., a "trap door" device). This malware warranty shall apply until the later of the end of the warranty period specified in the order or one (1) year after the date on which the Software is accepted by the State.

6.4 General. No warranties provided by the Reseller or Licensor will be invalidated by the failure of the State to install or otherwise use an available Software update (e.g., a new version or release).

## 7. Limitation Of Liability

7.1 Limitation of State's Liability. The State shall have no liability except as specifically provided in this Rider. In no event will the State be liable to the Licensor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Rider otherwise.

7.2 Limitation of Licensor's Liability. In accordance with Tenn. Code Ann. § 12-3-701, Licensor's liability for all claims arising under this Rider or the EULA shall be limited to an amount equal to two (2) times the total fees paid under the total of any purchase orders issued by the State under the Contract or otherwise paid by the State under the Contract for Licensor's Software, cloud services, and associated services, or the sum of one million dollars ($1,000,000), whichever is greater. Except as set forth below, in no event will the Licensor be liable to the State or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under the EULA, unless such damages are insured by any insurance coverages required by the EULA or would have been covered had the required insurance been purchased or maintained. PROVIDED THAT in no event shall this Section limit the liability of Licensor for: (i) intellectual property or any Licensor indemnity obligations for infringement for third-party intellectual property rights; ii) if applicable, any claims covered by any specific provision in the Contract providing for liquidated damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death.

**8. Indemnification for Intellectual Property Infringement**

Licensor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement that arises from or is associated with the Software or associated services. In any such claim or action brought against the State, Licensor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and Licensor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give Licensor notice of any such claim or suit, however, the failure of the State to give such notice shall only relieve Licensor of its obligations under this Section to the extent Licensor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant Licensor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

**9. No Additional Terms Permitted**

No online terms and conditions that are incorporated by reference in the EULA will be binding on Licensee. In addition, no shrink-wrap, click-wrap or other end user terms and conditions that are embedded in or provided with any Software or service are binding on Licensee, even if use of the Software requires an affirmative acceptance of those terms. Licensor shall fill all orders submitted by Reseller or the State under the Contract. No purchase order, invoice, or other documents associated with any sales, orders, or supply of any Software or service under the Contract shall contain any terms or conditions conflicting with any provision of this Rider.

**10. No Portion of this Agreement may be Changed Unilaterally**

No portion of the Rider or the EULA may be materially changed unilaterally. To be valid, any amendment that materially changes this Rider or the EULA must be in writing and signed by the parties. Non-material changes to the EULA shall be effective upon providing notice to the State of the changes. Any provision in the EULA to the contrary is deemed to conflict with this Rider and shall be null and void.

**11. Governing Law; Jurisdiction and Venue.**

This Rider and the EULA shall be governed by and construed in accordance with the laws of the State of Tennessee without regard to its conflict or choice of law rules. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Rider, the EULA, or the Contract. Licensor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Rider shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 407.

**12. <u>Fees</u>**

12.1 All fees and payments for License of Software or any services provided by Licensor under the EULA, this Rider, or the Contract shall be paid by State solely to Reseller. Licensor waives the right to collect any fees or payments directly from the State for any Software or services provided by Licensor under the Contract. Licensor's sole remedy shall be against Reseller, its Affiliates and assigns for any fees or payments owed for the State's for anything provided by Licensor under the EULA, this Rider, or the Contract. The State is not responsible for an early termination fee.

12.2 The State will not be liable for any unauthorized use, including fees and charges that may become due to Licensor as a result of that use.

**13. <u>Iran Divestment Act.</u>** The requirements of Tenn. Code Ann. § 12-12-101 et.seq., addressing contracting with persons with investment activities in Iran, shall be a material provision of this EULA. The Licensor agrees, under penalty of perjury, that to the best of its knowledge and belief that it is not on the list created pursuant to Tenn. Code Ann. § 12-12-106.

**14. <u>Miscellaneous</u>** Any provision in the EULA or any third party provider agreement containing the following shall be null, void, and unenforceable against the State: (i) any provision requiring the State to indemnify Licensor or any other entity; (ii) any provision regarding confidentiality obligations that are contrary to the Tennessee Public Records Act; (iii) any provision requiring the State to pay taxes or reimburse Licensor for tax payments; (iv) any provision requiring the State to submit to any alternative dispute resolution; (v) any provision allowing collection of attorneys fees or late payments against the State other than as allowed under the Tennessee Prompt Pay Act; Tenn. Code Ann. § 12-4-701, et seq.; (vi) any provision allowing equitable or injunctive relief against the State; and (vii) any provision that is illegal to include in a contract with the State of Tennessee, to enforce against the State of Tennessee, or otherwise contravenes Tennessee or federal law.

**15. <u>Comptroller Audit Requirements</u>**

15.1 Upon reasonable notice and at any reasonable time, the Licensor and Subcontractor(s) agree to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Licensor and all Subcontractors used by the Licensor. Licensor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Contract. Licensor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Licensor and Subcontractor(s) personnel for the purpose of performing the information technology control audit.

The information technology control audit may include a review of general controls and application controls. General controls are the policies and procedures that apply to all or a large segment of the Licensor's or Subcontractor's information systems and applications and include controls over security management, access controls, configuration management, segregation of duties, and contingency planning. Application controls are directly related to the application and help ensure that transactions are complete, accurate, valid, confidential, and available. The audit shall include the Licensor's and Subcontractor's compliance with the State's Enterprise Information Security Policies and all applicable requirements, laws, regulations or policies.

The audit may include interviews with technical and management personnel, physical inspection of controls, and review of paper or electronic documentation.

For any audit issues identified, the Licensor and Subcontractor(s) shall provide a corrective action plan to the State within 30 days from the Licensor or Subcontractor receiving the audit report.

Each party shall bear its own expenses incurred while conducting the information technology controls audit.

15.2 For any Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS) models provided by the Licensor where the State will use the Licensor's or Subcontractor's applications or data centers to store or process State financial or other data that is used for reporting through the State's Comprehensive Annual Financial Report or is used for demonstrating compliance with the requirements of Title 2, Code of Federal Regulations, Part 200, "Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards," the Licensor and Subcontractor shall be subject to an annual System and Organization Controls (SOC) 2 Type 2 examination engagement or a SOC 1 Type 2 examination engagement by a qualified and reputable CPA firm in accordance with the standards of the American Institute of Certified Public Accountants.

The scope of the SOC 2 Type 2 examination for SaaS models must include the security, availability, confidentiality, and processing integrity Trust Services Criteria. The scope of the SOC 2 Type 2 examination for IaaS and PaaS models must include the security, availability, and confidentiality Trust Services Criteria. The scope of the SOC 1 Type 2 examination must include a review of internal control over financial reporting that is relevant to the Licensor's and Subcontractor's scope of work.

The Licensor shall provide a complete, unredacted version of the SOC 1 Type 2 examination report and SOC 2 Type 2 examination report to the State upon request. For any examination issues or exceptions described in the SOC 1 Type 2 examination report or SOC 2 Type 2 examination report, the Licensor shall submit corrective action plans to the State within 30 days from the issuance of the examination reports.

In the event the CPA firm issues a modified opinion on the SOC examination report, meaning that the opinion is qualified, adverse, or disclaimed, the Licensor will immediately advise the State in writing of its plan to correct the issues that caused the modified opinion. The Licensor must demonstrate to the State that the issues have been corrected prior to the commencement of the next scheduled SOC examination.

If the scope of the most recent SOC examination report does not include all of the current State fiscal year, upon request from the State, the Licensor must provide to the State a letter from the Licensor or Subcontractor stating whether the Licensor or Subcontractor made any material changes to their control environment since the prior audit and, if so, whether the changes, in the opinion of the Licensor or Subcontractor, would negatively affect the auditor's opinion in the most recent SOC examination report. No additional funding shall be allocated for these audits as they are included in the Estimated Liability of this Contract.

The State and Comptroller of the Treasury must approve any exceptions to this requirement.

**16. Licensor Hosted Services Confidential Data, Audit, and Other Requirements**.

The following provisions shall only apply if an order expressly says that they apply to such order.

16.1 "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. The Licensor shall protect Confidential State Data as follows:

16.1.1 The Licensor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.

16.1.2 The Licensor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies.

16.1.3 The Licensor and the Licensor's processing environment containing Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization ("ISO") 27001; (ii) Federal Risk and Authorization Management Program ("FedRAMP"); or (2) be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants ("AICPA") for a System and Organization Controls for service organizations ("SOC") Type II audit. The State shall approve the SOC audit control objectives. The Licensor shall provide proof of current ISO certification or FedRAMP authorization for the Licensor and Subcontractor(s), or provide the State with the Licensor's and Subcontractor's annual SOC Type II audit report within 30 days from when the CPA firm provides the audit report to the Licensor or Subcontractor. The Licensor shall submit corrective action plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Licensor or Subcontractor.

If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Licensor must provide to the State a letter from the Licensor or Subcontractor stating whether the Licensor or Subcontractor made any material changes to their control environment since the prior audit and, if so, whether the changes, in the opinion of the Licensor or Subcontractor, would negatively affect the auditor's opinion in the most recent audit report.

No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Estimated Liability of this Contract.

Licensor shall meet all applicable requirements of the most current version of Internal Revenue Service Publication 1075.

Licensor shall meet requirements of current version of Minimum Acceptable Risk Standards for Exchanges ("MARS-E") controls.

16.1.3.1 If the order will involve CJIS data, or FTI data then the following shall apply in lieu of section 14.a.(3):

The Licensor shall maintain a Security Management Certification from the Federal Risk and Authorization Management Program ("FedRAMP"). A "Security Management Certification" shall mean written confirmation from FedRAMP that FedRAMP has assessed the Licensor's information technology Infrastructure, using a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, and has certified that the Licensor meets FedRAMP standards.

Information technology “Infrastructure” shall mean the Licensor’s entire collection of hardware, software, networks, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support information technology services. The Licensor shall provide proof of current certification annually and upon State request. No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Estimated Liability of this Contract.

16.1.3.2 If the order will contain FTI data, the following sentence also applies to section 14.a.(3)(a) (FedRAMP) language above:
Licensor shall meet all applicable requirements of the most current version of Internal Revenue Service Publication 1075.

16.1.3.3 If the order will involve CMS data, the following sentence also applies to section 14.a.(3)(a) language above:
Licensor shall meet requirements of current version of Minimum Acceptable Risk Standards for Exchanges (“MARS-E”) controls.

16.1.4 The Licensor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. “Processing Environment” shall mean the combination of software and hardware on which the Application runs. “Application” shall mean the computer code that supports and accomplishes the State’s requirements as set forth in this Contract. “Penetration Tests” shall be in the form of attacks on the Licensor’s computer system, with the purpose of discovering security weaknesses which have the potential to gain access to the Processing Environment’s features and data. The “Vulnerability Assessment” shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Licensor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.

16.1.5 Upon State request, the Licensor shall provide a copy of all Confidential State Data it holds. The Licensor shall provide such data on media and in a format determined by the State.

16.1.6 Upon termination of this Contract and in consultation with the State, the Licensor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology (“NIST”) Special Publication 800-88. The Licensor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

16.1.7 If the order will involve PCI data, the following shall apply:
Licensor shall be certified to host Payment Card Industry (“PCI”) data in accordance with the current version of PCI DSS (“Data Security Standard”), maintained by the PCI Security Standards Council.

16.2 Minimum Requirements

16.2.1 The Licensor and all data centers used by the Licensor to host State data, including those of all Subcontractors, must comply with the State’s Enterprise Information Security Policies as amended periodically. The State’s Enterprise Information Security Policies document is found at the following URL: https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html.

16.2.2 The Licensor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. “Operating System” shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

16.2.3 If the Application requires middleware or database software, Licensor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

16.3 Business Continuity Requirements. The Licensor shall maintain set(s) of documents, instructions, and procedures which enable the Licensor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:

16.3.1 "Disaster Recovery Capabilities" refer to the actions the Licensor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:

16.3.1.1 Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: The applicable RPO will be defined in each Order.

16.3.1.2 Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: The applicable RTO will be defined in each Order.

16.3.2 The Licensor and the Subcontractor(s) shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Licensor verifying that the Licensor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Licensor shall provide written confirmation to the State after each Disaster Recovery Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

16.3.3 The Licensor shall have the ability to provide base level protection against Layer 3 and Layer 4 Distributed Denial of Service volume based and protocol attacks such as SYN, UDP, and ICMP floods, DNS amplification and reflection attacks.

16.3.4 The Licensor shall have the ability to provide addition mitigation against Layer 7 Distributed Denial of Service attacks such as HTTP floods, WordPress XML-RPV Floods and Slowloris attacks.

16.4 In the event of a cyber breach, the Licensor will allow the State to communicate directly with the Licensor's technical staff and any forensics experts who are assisting the Licensor with the breach analysis.

ACKNOWLEDGED AND ACCEPTED BY:
Licensor: ________________________
Name: __________________________
Title: ___________________________
Date: ___________________________
Email: ___________________________

Licensee: State of Tennessee_______
Name:___________________________
Title: ___________________________
Date:____________________________
Email: CPO.SWC@tn.gov_________